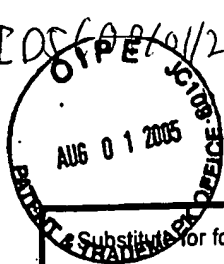


105/005/01/2005 (om 07/28/2005)



PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)			Complete if Known	
			Application Number	10/005,105
			Filing Date	December 3, 2001
			First Named Inventor	Paul C. Kocher
			Group Art Unit	2132
			Examiner Name	Justin T. Darrow
Sheet 1 of 3	Attorney Docket No.r	44424162-8721		

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
JD		4,211,919 A	07/08/1980	Michel Ugon	235/487
JD		4,295,041 A	10/13/1981	Michel Ugon	234/1107
JD		4,916,333 A	04/10/1990	Jacek Kowalski	307/206.5
JD		4,932,053 A	06/05/1990	Serge Fruhauf et al.	380/4
JD		5,297,201 A	03/22/1994	John H. Dunlavy	380/6
JD		5,412,723 A	05/02/1995	Ran Canetti et al.	380/21
JD		5,636,157 A	06/03/1997	James H. Hesson et al.	364/788
JD		5,991,415 A	11/23/1999	Adi Shamir	380/30
JD		6,434,238 B1	08/13/2002	David Chaum et al.	380/45
JD		6,698,662 B1	03/02/2004	Nathalie Feyt et al.	235/492

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Country Code ³	Number ⁴ Kind Code ⁵ (if known)			

Examiner Signature	<i>Justin Darrow</i>	Date Considered	09/29/2005
--------------------	----------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

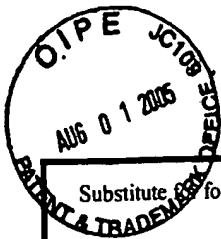
Substitute for form 1449B/PTO			Complete if Known	
			Application Number	10/005,105
INFORMATION DISCLOSURE STATEMENT BY APPLICANT			Filing Date	December 3, 2001
			First Named Inventor	Paul C. Kocher
			Group Art Unit	2132
			Examiner Name	Justin T. Darrow
(use as many sheets as necessary)			Attorney Docket No.	44424162-8721
Sheet	2	of	3	

OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
JP		BACK, Adam, "Non-Interactive Forward Secrecy" 09/06/1996	
JP		BELL, Jim, "Spread-Spectrum Computer Clock?" Google Beta Groups	
JP		BELLARE et al., "Optimal Asymmetric Encryption", Advanced Networking Laboratories, 1998, pp 92-111, Springer-Verlag, U.S.A.	
JP		BELLARE et al, "The Exact Security of Digital Signatures- How to Sign with RSA and Rabin", Advances in Cryptology - Eurocrypt 96 Proceedings, Lecture Notes in Computer Science, Vol. 1070, , pp 1-16, U. Maurer ed., Springer-Verlag, 1996	
JP		BELLARE et al, "Forward Integrity For Secure Audit Logs", pp 1-16, November 23, 1997, U.S.A.	
JP		FRANKEL et al., "Optimal-Resilience Proactive Public-Key Cryptosystems" IEEE Symposium on Foundations of Computer Science, 1997	
JP		FRANKEL et al., "Proactive RSA", Lecture Notes in Computer Science, 1996	
JP		HERZBERG et al, "Proactive Public Key and Signature Systems", ACM Conference on Computer and Communications Security, 1996	
Examiner Signature	Justin Darrow		Date Considered 09/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Substitute form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary) Sheet <u>3</u> of <u>3</u>		Complete if Known	
		Application Number	10/005,105
		Filing Date	December 3, 2001
		First Named Inventor	Paul C. Kocher
		Group Art Unit	2132
		Examiner Name	Justin T. Darrow
		Attorney Docket No.	44424162-8721
OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
JD		MENZES et al, "Pseudorandom Bits and Sequences", Handbook of Applied Cryptography, CRC Press, Chapter 5, pp 169-190, 1996	
JD		MENZES et al, "Efficient Implementation", Handbook of Applied Cryptography, CRC Press, Chapter 14, pp 591-634, 1996	
JD		RIVEST, Ronald, "Timing Cryptanalysis of RSA, DH, DDS" Google Beta Groups	
Examiner Signature	Justin Darrow		Date Considered 09/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)			Application Number	10/005,105	
			Filing Date	December 3, 2001	
			First Named Inventor	Paul C. Kocher	
			Group Art Unit	2132	
			Examiner Name	Justin T. Darrow	
Sheet	1	of	1	Attorney Docket Number	44424162-8721

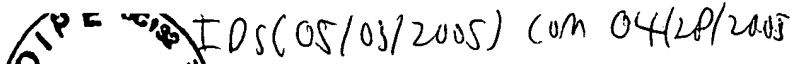
U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ³
		Country Code ⁴ Number ⁴ Kind Code ⁵ (if known)				
		EP 90201136.0 A1	11/28/1990	Koninklijke PTT Nederland N.V.	4042 9/06	<input type="checkbox"/>
		WO 99/08411 A2	02/18/1999	Jonathan Stiebel	4044 1/06	<input type="checkbox"/>

Examiner Signature	Justin Darrow	Date Considered	09/28/2005
-----------------------	---------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

(use as many sheets as necessary)

Sheet	1	of	2
-------	---	----	---

Complete if Known

Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

class/subclass

FOREIGN PATENT DOCUMENTS

Cross Subcell

Austin Sano

09/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 509. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Please type a plus sign (+) inside this box ☐

Under the Paperwork Reduction Project of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

PTO/SB/08B (08-00)

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Complete if Known			
		Application Number	10/005,105		
		Filing Date	December 3, 2001		
		First Named Inventor	Paul C. Kocher		
		Group Art Unit	2132		
		Examiner Name	Justin T. Darrow		
Sheet	2	of	2	Attorney Docket Number	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²
JP		KOCHER, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", 08/18/1996 XP000626590.	

Examiner Signature	Justin Darrow	Date Considered	09/29/2005
-------------------------------	---------------	----------------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

0m 12/13/12
O I P E J C I S N
JAN 05 2005
Reduction Act of 1995, no. 199
PATENT & TRADEMARK

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Complete if Known

Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	not yet known Justin T. Darrow
Attorney Docket Number	44424162-8721

Sheet	1	of	1
-------	---	----	---

Class / 546 class

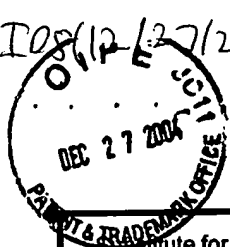
FOREIGN PATENT DOCUMENTS

Examiner Signature	<i>Austin Brown</i>	Date Considered	08/29/2005
--------------------	---------------------	-----------------	------------

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

108(12/27/2004) COM (12/21/2004)



PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)				Complete if Known		
				Application Number	10/005,105	
Sheet		1	of	1	Examiner Name	not yet known Justin T. Danner
					Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
JD		5,944,833 A	08/31/1999	Ugon	713 / 460

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ³
		Country Code ⁴ Number ⁴ Kind Code ⁵ (if known)				
JD		EP0826169B1	12/9/1997	Ugon	606 F 1/04	
JD		EP1064752B1	23/09/1999	Salle	104 L 9/06	
JD		EP1204948B1	1/2/2001	Leydier	606 K 19/073	

Examiner Signature	Justin Danner	Date Considered	09/29/2005
--------------------	---------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

705611/08/2004)(0M 11/03/2004

NOV 9 2004

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	10/005,105
				Filing Date	December 3, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
				Examiner Name	not yet known Justin T. Darrow
Sheet	1	of	2	Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
JD		* 4,107,458 A	01/08/1978	Constant	170/22
JD		*4,139,839 A	01/02/1979	Fletcher et al.	340/34700
JD		* 4,569,052 A	04/02/1986	Cohn et al.	371/138
JD		*4,605,921 A	08/01/1998	Riddle et al.	340/34700
JD		*5,144,667 A	09/01/1992	Pogue et al.	300/45
JD		* 5,159,632 A	10/27/1992	Crandall	300/20
JD		* 5,511,123 A	04/23/1996	Adams	300/29
JD		* 5,551,013 A	08/27/1996	Beausoleil et al.	395/500
JD		*5,559,890 A	09/09/1996	Obermeire et al.	300/40
JD		* 5,664,017 A	09/02/1997	Gressel et al.	300/30
JD		* 5,710,834 A	01/01/1998	Rhoads	302/232
JD		* 5,892,829 A	04/06/1999	Aiello et al.	300/25
JD		* 5,982,900 A	11/09/1999	Ebihara et al.	300/30

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)				
JD		EP 0 660 562 A2	06/28/1995	General Instrument Corporation of Delaware	4042 9/100	<input type="checkbox"/>
						<input type="checkbox"/>

Examiner Signature	Justin Darrow	Date Considered	09/29/2005
-----------------------	---------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Please type a plus sign (+) inside this box ☒

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitute for form 1449B/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)		Application Number	10/005,105
		Filing Date	December 3, 2001
		First Named Inventor	Paul C. Kocher
		Group Art Unit	2132
		Examiner Name	not yet known Justin T. Brown
Sheet 2 of 2	Attorney Docket Number	44424162-8721	

OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
J		LACY, J. et al., "CryptoLib Version 1.1", File Bigpow.c from CryptoLib, United States, November 1999.	
JP		"File NN.C from RSAFEF", RSA Laboratories, a division of RSA Data Security, Inc., United States, 1991.	
JP		WAYNER, P., "Code Breaker Crack Smart Cards, Digital Safe", New York Times, United States, 06/22/98, on the World Wide Web at: http://www.nytimes.com/library/tech/98/06/biztech/articles/22card.html	

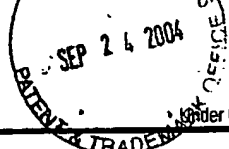
Examiner Signature	<i>Justin T. Brown</i>	Date Considered	09/29/2005
--------------------	------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

DOF 09/24/2004 COM 09/22/2004



PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)			Complete if Known		
			Application Number	10/005,105	
			Filing Date	December 3, 2001	
			First Named Inventor	Paul C. Kocher	
			Group Art Unit	2132	
			Examiner Name	not yet known <i>Justin T. Darrin</i>	
			Attorney Docket Number	44424162-8721	
Sheet	1	of	3	RECEIVED SEP 27 2004 Technology Center 2100	

U.S. PATENT DOCUMENTS						Class/Subclass
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	
		Number-Kind Code ² (if known)				
<i>JD</i>	AA	US-4,203,166 A	05/13/1980	Ehram et al.	375/2	
<i>JD</i>	AB	US-4,214,126 A	07/22/1980	Wipff	179/1.5M	
<i>JD</i>	AC	US-4,243,890 A	01/06/1981	Miller et al.	250/551	
<i>JD</i>	AD	US-5,241,598 A	08/31/1993	Raith	380/21	
<i>JD</i>	AE	US-5,297,201 A	03/22/1994	Dunlavy	380/6	
<i>JD</i>	AF	US-5,341,423 A	08/23/1994	Nossen	380/6	
<i>JD</i>	AG	US-5,369,706 A	11/29/1994	Latka	380/23	
<i>JD</i>	AH	US-5,412,379 A	05/02/1995	Waraska et al.	340/825-72	
<i>JD</i>	AI	US-5,420,925 A	05/30/1995	Michaels	380/23	
<i>JD</i>	AJ	US-5,544,086 A	08/06/1996	Davis et al.	364/408	
<i>JD</i>	AK	US-5,552,776 A	09/03/1996	Wade et al.	340/825.31	
<i>JD</i>	AL	US-5,559,887 A	09/24/1996	Davis et al.	380/24	
<i>JD</i>	AM	US-5,600,324 A	02/04/1997	Reed et al.	341/176	
<i>JD</i>	AN	US-5,633,930 A	05/27/1997	Davis et al.	380/28	
<i>JD</i>	AO	US-5,733,047 A	03/31/1998	Furuta et al.	384/43	
<i>JD</i>	AP	US-5,761,306 A	06/02/1998	Lewis	347/22	

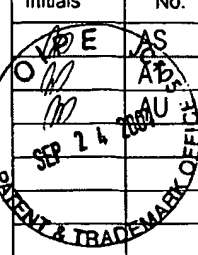
FOREIGN PATENT DOCUMENTS							C 1255/5a5c 1a11
Examiner Initials*	Cite No. ¹	Foreign Patent Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶	
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)					
JD	AQ	EP 0 529 261 A2	03/03/1993	IBM Corp.	H 04 L 9/08	<input type="checkbox"/>	
JD	AR	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp.	H 04 L 29/06	<input type="checkbox"/>	
						<input type="checkbox"/>	
						<input type="checkbox"/>	
						<input type="checkbox"/>	

Examiner Signature <i>Justin Darrin</i>	Date Considered 09/29/2005
---	----------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (use as many sheets as necessary)			Complete if Known		
			Application Number	10/005,105	
			Filing Date	December 3, 2001	
			First Named Inventor	Paul C. Kocher RECEIVED	
			Group Art Unit	2132	
Examiner Name	Not yet know SEP 27 2004				
Attorney Docket Number	44424162-8721				
Sheet	2	of	3		

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
	AS	US-5,778,065 A	07/07/1998	Hauser, et al.	380/21
	AB	US-5,796,836 A	08/18/1998	Markham, Thomas R.	380/28
	AU	US-5,995,629 A	11/30/1999	Reiner	380/50

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ Number ⁴ Kind Code ⁵ (if known)				
						<input type="checkbox"/>
						<input type="checkbox"/>
						<input type="checkbox"/>
						<input type="checkbox"/>
						<input type="checkbox"/>
						<input type="checkbox"/>

Examiner Signature	<i>Justin Brown</i>	Date Considered	09/29/2005
-----------------------	---------------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Best Available Copy

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Please type a plus sign (+) inside this box ☐

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitute for form 1449B/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known

Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	not yet known Justin T. Darrow
Attorney Docket Number	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
AP	AV	American National Standards for Financial Services, secretariat - American Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key Management," approved April 6, 1992, American National Standards Institute; pgs. 1-71	
AP	AW	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127	
AP	AX	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical University Munich, 1998; pgs. 31-48	
AP	AY	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure Your Wireless Designs", 01/18/96; pgs. 57-68	
AP	AZ	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt 91, 1991; pgs. 453-460	
AP	BA	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994, Chapter III; pgs. 53-77	
AP	BB	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91, 1991; pgs. 17-38	
AP	BC	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful Adversary?" 1999	
AP	BD	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6	
AP	BE	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories, Bulletin, Number 2, January 23, 1996	

Examiner Signature	<i>Justin Darrow</i>	Date Considered	09/29/2005
--------------------	----------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Best Available Copy

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

028420-0012CIP

10/005,105

P. Kocher et al.

FILING

December 3, 2001

GROUP

2132
Unassigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JD	4,200,770 A	4/1980	Hellman et al.	178	22	09/06/1977
JD	4,405,829 A	9/1983	Rivest et al.	178	22.1	12/14/1977
JD	4,759,063 A	7/1988	Chaum	380	30	08/22/1983
JD	4,799,258 A	1/1989	Davies	380	21	02/07/1985
JD	4,905,176 A	2/1990	Schulz	364	717	10/28/1988
JD	4,908,038 A	3/1990	Matsumura et al.	902	5	10/27/1988
JD	5,136,646 A	8/1992	Haber et al.	380	49	03/08/1991
JD	5,297,207 A	3/1994	Degele	380	46	05/24/1993
JD	5,401,950 A	3/1995	Yoshida	235	487	02/19/1992
JD	5,404,402 A	4/1995	Sprunk	380	4	12/21/1993
JD	5,539,827 A	07/1996	Liu	380	37	04/05/1995

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JD		"Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, U.S. Department of Commerce, National Institute of Standards and Technology, January 1994, pp. 1-53.
JD		RSA Data Security, RSAREF Cryptographic Toolkit Source Code, File R_RANDOM.C, available from ftp://ftp.rsa.com, created 1991, pp. 1-2.

EXAMINER

Justin Banger

DATE CONSIDERED

08/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

ATTY DOCKET NO.

028420-0012CIP

SERIAL NO.

10/005,105

P. Kocher et al.

FILING

December 3, 2001

GROUP

2132
~~Unassigned~~

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JD	5,546,463 A	8/1996	Caputo et al.	380	25	07/12/1996
JD	5,663,896 A	9/1997	Aucsmith	395	187.01	09/22/1997
JD	5,664,017 A	9/1997	Gressel et al.	380	30	05/08/1998
JD	5,727,063 A	3/1998	Aiello et al.	380	46	11/27/1998
JD	5,778,074 A	7/1998	Garcken et al.	380	37	06/28/1996
JD	5,812,669 A	9/1998	Jenkins et al.	380	25	07/18/1995
JD	5,835,599 A	11/1998	Buer	380	29	04/15/1996
JD	5,838,795 A	11/1998	Mittenthal	380	28	07/07/1997
JD	5,848,159 A	12/1998	Collins et al.	380	30	01/16/1997
JD	5,991,415 A	11/1999	Shamir	380	30	05/12/1997
JD	6,041,122 A	03/2000	Graunke et al.	380	21	02/27/1998

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JD	M. Bellare et al., "Incremental Cryptography: The Case of Hashing and Signing" in: Desmedt, Y., Advances in Cryptology - Crypto 94 Proceedings (Springer-Verlag, 1994) pp. 216-233.
JD	Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in: Koblitz, N., Advances in Cryptology - Crypto '96 (Berlin, Springer, 1996), pp. 104-113.

EXAMINER

Justin Zarrow

DATE CONSIDERED

09/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

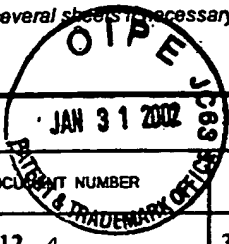
ATTY DOCKET NO.
028420-0012CIP

SERIAL NO.
10/005,105

P. Kocher et al.

FILING
December 3, 2001

GROUP
2/32
Unassigned



U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JP	6,041,412 A	3/2000	Timson, et al.	713	200	11/14/1997
JP	6,049,613 A	4/2000	Jakobsson	380	47	01/13/1998
JP	6,064,724 A	5/2000	Kelly	379	92.04	11/22/1996
JP	6,064,740 A	5/2000	Curiger et al.	380	265	11/12/1997
JP	6,069,954 A	5/2000	Moreau	380	28	05/09/1997

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JP		Schneier, Bruce, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, Inc. 10/18/95, pp. 34-41, 390-392 and 480-481.
JP		Krawczyk, H., et al., "HMAC: Keyed-Hashing for Message Authentication," Network Working Group Request for Comments RFC 2104, February 1997, pp. 1-11.

EXAMINER

Justin Zenger

DATE CONSIDERED

08/29/2005

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

